

**What Is Claimed Is:**

1           1.       A method for managing a database system, comprising:  
2           receiving a command to perform an administrative function involving an  
3           object defined within the database system;  
4           determining if the object is a sensitive object that is associated with  
5           security functions in the database system;  
6           if the object is not a sensitive object, and if the command is received from  
7           a normal database administrator for the database system, allowing the  
8           administrative function to proceed; and  
9           if the object is a sensitive object, and if the command is received from a  
10          normal system administrator, disallowing the administrative function.

1           2.       The method of claim 1, further comprising:  
2           receiving a request to perform an operation on a data item in the database  
3           system;  
4           if the data item is a sensitive data item containing sensitive information  
5           and if the request is received from a sensitive user who is empowered to access  
6           sensitive data, allowing the operation to proceed if the sensitive user has access  
7           rights to the data item; and  
8           if the data item is a sensitive data item and the request is received from a  
9           normal user, disallowing the operation.

1           3.       The method of claim 2, wherein if the data item is a sensitive data  
2           item, if the operation is allowed to proceed, and if the operation involves retrieval  
3           of the data item, the method further comprises decrypting the data item using an  
4           encryption key after the data item is retrieved.

1           4.       The method of claim 3, wherein the encryption key is stored along  
2       with a table containing the data item.

1           5.       The method of claim 4, wherein the encryption key is stored in  
2       encrypted form.

1           6.       The method of claim 1, wherein the sensitive object can include  
2       one of:  
3           a sensitive table containing sensitive data in the database system;  
4           a sensitive row within a table in the database system, wherein the sensitive  
5       row contains sensitive data; and  
6           an object that represents a sensitive user of the database system who is  
7       empowered to access sensitive data.

1           7.       The method of claim 1, wherein if the object is not a sensitive  
2       object, and if the command to perform the administrative function is received  
3       from a security officer, the method further comprises allowing the security officer  
4       to perform the administrative function on the object.

1           8.       The method of claim 1,  
2       wherein the database system includes a number of sensitive data items;  
3       and  
4       wherein only specific sensitive users are allowed to access a given  
5       sensitive data item.

1           9.     A computer-readable storage medium storing instructions that  
2     when executed by a computer cause the computer to perform a method for  
3     managing a database system, the method comprising:  
4         receiving a command to perform an administrative function involving an  
5     object defined within the database system;  
6         determining if the object is a sensitive object that is associated with  
7     security functions in the database system;  
8         if the object is not a sensitive object, and if the command is received from  
9     a normal database administrator for the database system, allowing the  
10    administrative function to proceed; and  
11         if the object is a sensitive object, and if the command is received from a  
12    normal system administrator, disallowing the administrative function.

1           10.    The computer-readable storage medium of claim 9, wherein the  
2    method further comprises:  
3         receiving a request to perform an operation on a data item in the database  
4    system;  
5         if the data item is a sensitive data item containing sensitive information  
6    and if the request is received from a sensitive user who is empowered to access  
7    sensitive data, allowing the operation to proceed if the sensitive user has access  
8    rights to the data item; and  
9         if the data item is a sensitive data item and the request is received from a  
10   normal user, disallowing the operation.

1           11.    The computer-readable storage medium of claim 10, wherein if the  
2    data item is a sensitive data item, if the operation is allowed to proceed, and if the

3 operation involves retrieval of the data item, the method further comprises  
4 decrypting the data item using an encryption key after the data item is retrieved.

1 12. The computer-readable storage medium of claim 11, wherein the  
2 encryption key is stored along with a table containing the data item.

1 13. The computer-readable storage medium of claim 12, wherein the  
2 encryption key is stored in encrypted form.

1 14. The computer-readable storage medium of claim 9, wherein the  
2 sensitive object can include one of:  
3 a sensitive table containing sensitive data in the database system;  
4 a sensitive row within a table in the database system, wherein the sensitive  
5 row contains sensitive data; and  
6 an object that represents a sensitive user of the database system who is  
7 empowered to access sensitive data.

1 15. The computer-readable storage medium of claim 9, wherein if the  
2 object is not a sensitive object, and if the command to perform the administrative  
3 function is received from a security officer, the method further comprises allowing  
4 the security officer to perform the administrative function.

1 16. The computer-readable storage medium of claim 9,  
2 wherein the database system includes a number of sensitive data items;  
3 and  
4 wherein only specific sensitive users are allowed to access a given  
5 sensitive data item.

1           17.    An apparatus for managing a database system, comprising:  
2           a command receiving mechanism that is configured to receive a command  
3           to perform an administrative function involving an object defined within the  
4           database system;  
5           an execution mechanism that is configured to,  
6                    determine if the object is a sensitive object that is  
7                    associated with security functions in the database system,  
8                    allow the administrative function to proceed, if the object is  
9                    not a sensitive object, and if the command is received from a  
10                  normal database administrator for the database system, and to  
11                  disallow the administrative function, if the object is a  
12                  sensitive object, and if the command is received from a normal  
13                  system administrator.

1           18.    The apparatus of claim 17,  
2           wherein the command receiving mechanism is configured to receive a  
3           request to perform an operation on a data item in the database system;  
4           wherein the execution mechanism is configured to,  
5                    allow the operation to proceed, if the data item is a  
6                    sensitive data item, if the request is received from a sensitive user  
7                    who is empowered to access sensitive data, and if the sensitive user  
8                    has access rights to the data item, and to  
9                    disallow the operation, if the data item is a sensitive data  
10                  item, and if the request is received from a normal user.

1           19.     The apparatus of claim 18, further comprising a decryption  
2     mechanism, wherein if the data item is a sensitive data item, if the operation is  
3     allowed to proceed, and if the operation involves retrieval of the data item, the  
4     decryption mechanism is configured to decrypt the data item using an encryption  
5     key after the data item is retrieved

1           20.     The apparatus of claim 19, wherein the encryption key is stored  
2     along with a table containing the data item.

1           21.     The apparatus of claim 20, wherein the encryption key is stored in  
2     encrypted form.

1           22.     The apparatus of claim 17, wherein the sensitive object can include  
2     one of:  
3             a sensitive table containing sensitive data in the database system;  
4             a sensitive row within a table in the database system, wherein the sensitive  
5     row contains sensitive data; and  
6             an object that represents a sensitive user of the database system who is  
7     empowered to access sensitive data.

1           23.     The apparatus of claim 17, wherein if the object is not a sensitive  
2     object, and if the command to perform the administrative function is received  
3     from a security officer, the execution mechanism is configured to allow the  
4     security officer to perform the administrative function.

1           24.     The apparatus of claim 17,

- 1            wherein the database system includes a number of sensitive data items;
- 2    and
- 3            wherein only specific sensitive users are allowed to access a given
- 4    sensitive data item.